PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of: Menno Anne Treffers et al.	
US Application No. 09/930,654	Examiner: Popham, Jeffery D.
Confirmation No. 1920	
Filed: August 15, 2001	Group Art Unit: 2137
Attorney Docket No. 93418.000047	

For: METHOD AND DEVICE FOR CONTROLLING DISTRIBUTION AND USE OF DIGITAL WORKS

September 20, 2006

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF IN REPLY TO EXAMINER'S ANSWER MAILED JULY 20, 2006

Appellants submit the following remarks in reply to the Examiner's Answer (hereinafter "the Answer") mailed July 20, 2006, in the on-going appeal in the above-captioned application.

Status of the Claims

Claims 1 through 13 are pending in the application. All of the claims have been finally rejected, and are being appealed herein. A clean, double-spaced copy of the claims on appeal was provided as Appendix A in the Appeal Brief filed May 10, 2006.

Grounds of Rejection to be Reviewed on Appeal

1. Claims 1 and 3-13 stand rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Published Patent Application No. 2001/0042043 (Shear et al.) in view of United States Patent No. 6,226,618 (Downs et al.) and United States Patent No. 5,892,900 (Ginter et al.).

2. Claim 2 also stands rejected under 35 U.S.C. §103(a), as unpatentable over Shear et al. in view of Downs et al. and Ginter et al., and further in view of United States Patent No. 6,064,751 (Smithies et al).

Argument

In compliance with the provisions of 37 CFR 41.41, this reply brief contains no new or non-admitted amendment and no new or non-admitted affidavit or other evidence. To the extent that this Reply attempts only to address the points raised in the Answer, each of the claims on appeal is not addressed in the detail in which they were originally addressed in the Appeal Brief. To the extent that arguments presented in the Appeal Brief are not re-presented herein, Appellants hereby incorporate those arguments by reference. In no way should this Reply be construed to limit the arguments presented in the Appeal Brief. Similarly, in no way should Appellants' rights to argue any of the claims or claim features be limited by this Reply.

The contentions raised by the Examiner in the Answer will be addressed below generally in order.

Initially, the Answer seems to indicate in at least two locations that terms of claim 1 were mischaracterized in the Appeal Brief. To clarify any ambiguity in this regard, Appellants submit that claim 1 recites a method for controlling distribution and use of a digital work. *Inter alia*, claim 1 features a step of "changing a hidden information stored in a hidden channel and used for encrypting or verifying [] usage right information when said usage right information has changed."

The Answer again asserts that Shear et al. teaches that hidden information is used for encrypting or verifying usage right information. Appellants disagree. Page 15, at paragraphs [0216]-[0218], describes that an encrypted key block 208 and hidden keys 210 are stored on a disk 100. The key block 208 contains different cryptographic keys for decrypting different properties 200 and/or metadata blocks 202 and/or different portions of the same property and/or metadata block. That is, the key block 208 contains keys for decrypting content stored on the disk. The hidden keys 210 are stored on the disk 100 at a "not normally accessible" location and are used to decrypt the encrypted key block 208. Accordingly, Shear et al. teaches that hidden keys are used to decrypt keys that are used to decrypt content. In paragraph [0214], Shear et al. also teaches that "disk 100 may store control rules in the form of a control set 204—which may be packaged in the form of one or more secure containers 206." The encrypted key block 208 may be included within or as a part of the secure container 206. Paragraph [0216].

Based on this disclosure, the Answer takes the position that when the encrypted key block is stored in a secure container, "the hidden keys will decrypt the container itself." The

Answer further concludes from this disclosure that "[i]f the encrypted key block is outside the secure container, the hidden keys will decrypt the encrypted key block, and those keys from the key block will decrypt the secure container." Examiner's Answer, Page 11.

Appellants disagree. Shear et al. is understood only to teach that hidden keys are used to decrypt an encrypted key block, and the keys in the key block are used to access protected content information. According to Shear et al., the encrypted key block may be placed in a secure container that also contains control rules, but there is only disclosure of using hidden keys to gain access to protected content—not to gain access to the secure container.

Nevertheless, even assuming, *arguendo*, that the hidden keys stored are to gain access to the protected content, the hidden keys are understood to be used only for decryption. That is, and the examiner agrees, that the hidden keys "will decrypt an encrypted key block" or "will decrypt the secure container." Examiner's Answer, page 10. As previously asserted, the hidden keys are not used to encrypt or verify usage right information, as set forth in the claims at issue. For example, in one embodiment of Appellants' invention discussed in the substitute specification beginning at paragraph [0041], a key-locker update and encryption unit stores a key-locker key in a hidden channel of an optical disc and uses the key-locker key to encrypt a key locker table KLT storing usage right information. In another embodiment of the invention, as discussed at paragraphs [0049]-[0050] of the substitute specification, a key locker update and verification unit may store a checksum in the hidden channel, and manipulation of the key-locker table KLT can be verified by the key-locker update and verification unit using the hidden checksum.

The Answer also asserts that Shear et al. contemplates storing keys on a player to decrypt encrypted keys on a medium. Appellants agree, but again submit that storing keys on a player to decrypt encrypted keys on a medium is distinct from information stored in a hidden channel and used for encrypting or verifying usage right information. Moreover, Appellants note that when the keys are stored on the player, there is no indication that the keys are hidden.

Downs et al. teaches marking content at a content provider with copy/play code; scrambling the content before transmitting same to an end-user device; generating a scrambling key for each content item; hiding the key, after encrypting, in the end-user device; and upon access to the content, updating copy/play code.

Ginter et al. relates to a virtual distribution environment (VDE). The cited portion of Ginter et al. is understood to deal mainly with VDE objects 300 and related logical object structures 800 for the VDE objects 300. These concepts are discussed in more detail from column 134, line 11, to column 136, line 59, of Ginter et al. As discussed therein, "[e]ach logical object structure 800 may also include a 'private body' 806 containing or referencing a set of methods 1000 (i.e., programs or procedures) that control use and distribution of the object 300... Methods 1000 perform the basic function of defining what users (including, where appropriate, distributors, client administrators, etc.) can and cannot do with an object 300." Col. 135, ll. 35-38. For example, the methods may define unlimited viewing for a set period of time.

The logical object structure 800 may also include one or more permission records 808 specifying methods or combinations of methods that must be used to access or otherwise use the object or its contents. The permission records 808 may include key blocks 810 that store decryption keys for accessing the content of the encrypted content stored in the object 300. The permission records 808 and key blocks 810 are frequently distributed electronically, using secure communications techniques controlled by VDE nodes of the sender and receiver. Accordingly, permission records 808 and key blocks 810 are stored on electronic appliances 600 of registered users. The permission records and key blocks 810 for each property can be encrypted with a private DES key stored in the secure memory of an SPU or can be encrypted with an end user's public key. The one or more keys used to encrypt each permission record or other management information record will be changed every time the record is updated (or after a certain one or more events). Alternatively, the keys may be "time aged," or a combination of "time aged" and event triggered may be used to change the encryption keys. According to Ginter et al., encryption keys should be updated, because "the longer a key is used, the greater the chance that it may be compromised but still in use to protect new information." Col. 212, ll. 44-46.

Thus, to sum up the cited documents, Shear et al. teaches hidden keys stored on a disk used for decrypting encrypted content also contained on the disk. Shear et al. also teaches that the encrypted content may be stored in a secure container with control rules. Downs et al. teaches updating content usage conditions associated with content stored in an end-user device whenever the end-user device accesses the content for playing and/or copying. Ginter et al. teaches providing permission records and key blocks having keys for accessing content, encrypting the

permission records and key blocks with a DES key or a public key, and changing the keys used to encrypt the permission records.

None of the references, however, teaches at least changing a hidden information stored in a hidden channel and used for encrypting or verifying usage right information when the usage right information has changed, as recited in independent claims 1 and 13. Moreover, none of the references teaches that a record carrier comprises a hidden channel not accessible by commercial reproducing devices, a hidden information being stored in the hidden channel, said hidden information being used for encrypting or verifying said usage right information and which is changed when usage right information has changed, as recited in independent claim 11.

Such features of the independent claims also would not have been obvious to one of ordinary skill in the art in light of the disclosures of the cited documents. For starters, it would not have been obvious to replace hidden keys used for decrypting content, as disclosed in Shear et al., with information used for encrypting or verifying content, as claimed. Moreover, it would not have been obvious to change the hidden keys when usage right information has changed.

At most, Shear et al. teaches hidden keys on a record carrier for decrypting information, and Ginter et al. teaches changing a key used to encrypt permission records. The key of Ginter et al. may be (i) a private DES key stored only in a secure memory of an SPU or (ii) an end user's public key, used for encrypting records. It would not have been obvious to one of ordinary skill in the art to replace the hidden keys of Shear et al., which are used for decrypting content, with the private DES key or the end user's public key, which are used to encrypt records. The keys serve distinctly different purposes, and there is no suggestion or motivation to replace the hidden keys of Shear et al., used for decrypting content, with keys for encrypting or verifying usage right information.

Thus, even if one of ordinary skill in the art would look to Ginter et al., it would not have been obvious to modify the hidden keys of Shear et al. used for decrypting content in the manner suggested by the Examiner. The Examiner seems to pick and choose portions of published documents to reconstruct the subject matter claimed in Appellants' application. Such hindsight reconstruction is not permissible. Moreover, this improper reconstruction would not be possible absent the teachings of Appellants' disclosure.

In addition to the foregoing, Appellants also again assert that one having ordinary skill in the art would not have looked to Ginter et al. and Downs et al. when faced with finding a

solution for combating a replay-attack. Independent claim 11, for example, recites a hidden channel on a record carrier storing hidden information for encrypting or verifying usage right information and changing that hidden information when usage right information has changed. Shear et al. indicates that keys for decrypting content information may be hidden on a medium. Shear et al. also contemplates storing decryption keys inside a player for decrypting content on the medium. However, there is no motivation in Shear et al. to look to either Downs et al. or Ginter et al. to modify in any manner keys hidden on a medium. Moreover, even if there was some motivation to change the hidden keys of Shear et al., one would presumably look to other record carrier art to determine how to change such hidden information hidden on the carrier. Downs et al. relates to end-user devices and Ginter et al. relates to virtual distribution environments.

The Answer also indicates that one would combine Ginter et al. with Shear et al. because "Ginter is [] discussed within Shear, teaching that portions of Ginter could be incorporated into Shear, as seen by paragraphs 332, 334, and 345 of Shear, as well as others." Examiner's Answer, page 11. However, nowhere does Shear et al. indicate that the "Ginter et al." referred to in Shear et al. is the publication relied upon by the Examiner. A search of the U.S. Patent and Trademark Office Records for patents having an inventor named Ginter returned 92 hits, while a similar search of published patent applications yielded 44 hits.

Conclusion

For the foregoing reasons, Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the rejection by the Examiner and mandate allowance of the claims.

Respectfully submitted,

Michael J. Didas Registration No. 55,112
Customer Number 23387
HARTER, SECREST & EMERY LLP
1600 Bausch & Lomb Place
Rochester, New York 14604
Telephone: 585-231-1411
Fax: 585-232-2152